3 Tipe Karyawan Penyebab Rentan Bahaya Siber

Riset dari Haystax Technology ditemukan fakta bahwa bahwa 74% perusahaan merasa rentan dengan ancaman orang dalam, sementara 56 persen profesional keamanan menyakini bahwa dalam setahun terakhir ancaman dari orang dalam atau insider semakin sering terjadi.

Bagi sebuah perusahaan, kejahatan dunia maya selalu diartikan sebagai ancaman yang datang dari luar atau faktor eksternal. Namun, anggapan itu tidak sepenuhnya benar, ancaman internal yang sering diabaikan atau kurang mendapat perhatian bisa menjadi ancaman yang lebih besar. Banyak perusahaan menyadari bahwa ancaman karyawan yang terpercaya dan terlatih bisa menjadi pusat kerentanan itu sendiri.

Kejahatan siber yang berkaitan dengan karyawan biasanya disebabkan oleh karyawan yang dendam, banyak juga terjadi akibat kelalaian, seperti mengabaikan peringatan, gagal mengikuti prosedur atau kesalahan manusia sederhana. Dari berbagai tingkat kesalahan yang terjadi ESET telah mengidentifikasi tiga tipe karyawan yang dapat menyebabkan pelanggaran data:

Pelanggaran Tidak Diketahui

Banyak kasus pelanggaran data disebabkan karena ketidaktahuan karyawan, karyawan tidak menyadari jika perbuatannya merupakan sebuah kesalahan yang bisa memberikan dampak yang sangat besar dan mempengaruhi kelangsungan hidup sebuah perusahaan.

Seperti kirim email ke alamat yang salah, biasanya ke penerima yang memiliki alamat email yang mirip, padahal email berisi data- data penting milik perusahaan. Kesalahan yang terkait dengan dokumen adalah beberapa penyebab umum dari pelanggaran data. Beberapa contoh di antaranya mencakup meneruskan informasi sensitif kepada penerima yang salah, mempublikasikan data pribadi ke server web publik, dan dengan sembarangan membuang data pekerjaan rahasia.

Peristiwa ini biasanya terjadi secara internal tanpa melibatkan pihak ketiga. Bila ini terjadi, peretas bisa menggunakan informasi tersebut sebagai pemerasan atau sebagai aset bagi kelompok mereka. Mereka juga bisa mengakses rekening bank dan dokumen lainnya yang terkait dengan keuangan.

Dengan kasus seperti ini, tidak mengherankan bahwa 74% dari mereka yang disurvei oleh Haystax paling memperhatikan pelanggaran data akibat unsur ketidaktahuan ini.

Ceroboh atau Lalai

Sebuah survei oleh Google pada tahun 2013 menemukan bahwa 25 juta peringatan Chrome diabaikan oleh 70,2% pengguna karena kurangnya pengetahuan teknis pengguna, sehingga membuat Google menyederhanakan bahasa yang digunakan dalam peringatan yang mereka berikan.

Banyak pengguna komputer malas membaca terkait pemberitahuan, warning atau setiap kali muncul jendela pop up, terutama sekali jika berkaitan dengan penguduhan dan instalasi software, karena seringkali penjahat siber menyembunyikan file lain untuk ikut diunduh atau instalasi sebagai syarat, dan biasanya pengguna dengan mudah accept permintaan tersebut tanpa pernah terlebih

dahulu membaca, yang akhirnya berakibat fatal.

Kelalaian lain yang umum dilakukan karyawan ceroboh adalah menyimpan file penting perusahaan di tempat yang bisa diakses oleh semua orang. Atau kelalaian lain seperti kehilangan laptop yang di dalamnya berisi data-data berharga perusahaan.

Kesengajaan

Jika kedua jenis penyebab di atas bisa diklasifikasikan sebagai human error, yang satu ini masuk ke dalam kategori kejahatan, misalnya karyawan atau mantan karyawan secara diam-diam mengumpulkan data perusahaan kemudian dijual ke pihak ketiga atau ke perusahaan saingan.

Ulah insider semacam ini biasanya disebabkan alasan dendam, ancaman atau tawaran uang dalam jumlah besar. Tipikal serangan seperti ini yang biasanya kemudian kurang diperhitungkan oleh perusahaan yang lebih fokus menghadapi serangan dari luar.

Langkah Pencegahan

Dengan dampak kebocoran data yang menyebabkan gangguan dan kerusakan pada bisnis, termasuk kerugian finansial dan pencemaran nama baik perusahaan, tidak mengherankan jika perusahaan terbuka untuk menemukan cara mengurangi dan membatasi penyalahgunaan komputer. Berikut ESET memberikan beberapa langkah strategis untuk menghadapi bahaya laten internal:

Meningkatkan kesadaran karyawan

Mungkin langkah paling logis bagi pengusaha adalah memastikan bahwa semua karyawan menyadari dampak potensial dari tindakan mereka, dan bagaimana menghindari kehilangan data yang tidak disengaja atau ketidaktahuan akibat lemahnya kesadaran keamanan karyawan. Penting juga untuk melibatkan semua karyawan dalam pelatihan yang sesuai, dan bukan hanya mereka yang terlibat langsung dengan TI.

Simpan informasi dengan aman

Menurut peneliti ESET Stephen Cobb: "Ada sejuta alasan untuk mengenkripsi data". Mengenkripsi data bisa menjadi bagian penting dalam mencegah kehilangan data. Dengan enkripsi, sekalipun data tercuri, pelaku tidak dapat menggunakannya apalagi untuk dijual.

Pantau data dan perilaku

Mengawasi penggunaan komputer dan perilaku individu membantu perusahaan tetap sadar dan mengidentifikasi aktivitas yang tidak biasa atau berisiko. Perangkat BOYD (Bring Your Own Device) yang beroperasi di banyak perusahaan juga harus dipantau dan dikendalikan dengan seksama. Bila diperlukan, software pengaman seperti Safetica Data Leak Prevention (Pencegah Kebocoran Data) dapat diimplementasikan untuk melakukan monitoring dan pemblokiran.